Bijlage I - Introductie: authenticatie en eID

In het Algemeen Overleg (AO) van 25 november 2015 is gevraagd uiteen te zetten hoe de pilots voor de gebruiker er uit gaan zien. Onder het kopje introductie staat dit beschreven. Daarnaast is in het AO toegezegd nadere informatie te verstrekken over:

- Privacybescherming voor gebruikers van inlogmiddelen
- Beveiliging en toegang
- Eisen aan publieke dienstverleners en private leveranciers
- Het publieke eID-middel
- Buitenlandse overheden (kunnen persoonsgegevens in handen komen van buitenlandse overheden)

Introductie

Overheden en bedrijven bieden mensen en organisaties in toenemende mate de mogelijkheid om diensten digitaal af te nemen. Ook de Nederlandse overheid en de Europese Commissie stimuleren een verdergaande dienstverlening via internet. De Nederlandse overheid wil dat burgers en bedrijven in 2017 hun zaken digitaal kunnen laten verlopen.

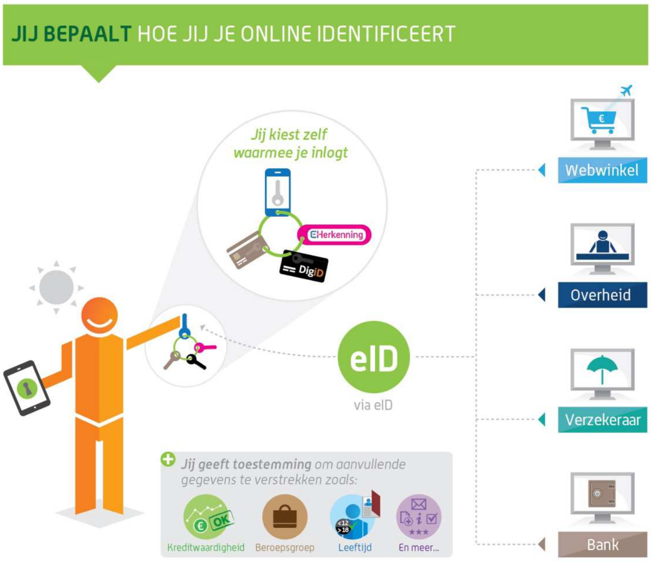
> De term 'eID' staat voor elektronische identiteit. Deze gebruik je als je bijvoorbeeld online gegevens over jezelf met een organisatie deelt.

Bij het beschikbaar stellen van digitale dienstverlening moet iedere organisatie een aantal vraagstukken op het terrein van geautoriseerde toegang oplossen. Het ontwikkelen van een eenduidige set regels en afspraken is dan een manier om die vraagstukken te uniformeren, zodat niet iedere organisatie 'het wiel opnieuw uitvindt'. Een dergelijke standaard gaat dus niet over de inhoud van de digitale diensten, maar bestaat uit een uniforme set van regels en afspraken voor geautoriseerde toegang tot digitale diensten. Het proces om online toegang te verkrijgen wordt ook wel aangeduid met de term authenticatie: het kunnen vaststellen van de identiteit van degene die zaken wil doen met een organisatie. Die identiteit kan overigens ook beperkt blijven tot het kunnen aantonen van alleen een bepaalde leeftijdsgrens.

Voor gebruikers leidt het huidige aanbod van toegangsvoorzieningen tot een uitgebreide 'digitale sleutelbos' van inlogmiddelen. Gebruikers moeten vaak een hele lijst aan gebruikersnaam en wachtwoorden onthouden, waarbij de wachtwoorden verplicht steeds ingewikkelder moeten worden samengesteld.







Voor de gebruiker biedt standaardisatie naast veiligheid ook vooral gebruiksgemak. Als de gebruiker een digitale dienst wil afnemen, kan hij bij organisaties zelf kiezen met welk middel hij zich identificeert. Zo kan hij één (of een beperkte set) inlogmiddel(en) gebruiken om veilig online zaken te doen met meerdere organisaties. Tevens geeft dat de mogelijkheid om de afhankelijkheid van één specifiek inlogmiddel (zo is er voor burgers in het publieke domein nu alleen DigiD) te beperken en een strategie te hebben waarin meerdere inlogmiddelen beschikbaar zijn om dienstverlening te ontsluiten, de zogenoemde multi-middelen strategie. Daarmee wordt een terugvaloptie bij calamiteiten gecreëerd.

Hoe gaat dat dan in de praktijk werken?

Een gebruiker kan zelf kiezen welk inlogmiddel hij gebruikt. Dat betekent dat een dienstaanbieder van te voren niet weet met welk middel een gebruiker zal inloggen. Dit model is vergelijkbaar met het iDEAL-model: de webwinkel weet ook niet van te voren met welke bank een gebruiker zal betalen. Dat betekent dat er een 'makelaarsfunctie' tussen de gebruiker en de dienstaanbieder is ingericht. Deze makelaars-functie regelt dat de gebruiker een keuze kan maken voor zijn inlogmiddel en dat er vervolgens een technische verbinding tussen de dienstaanbieder en de gekozen authenticatiedienst tot stand komt. De informatie die vervolgens door de authenticatiedienst wordt gegenereerd voor de dienstaanbieder, wordt zodanig versleuteld dat alleen de dienstaanbieder die informatie kan lezen. De makelaarsfunctie is alleen een logistieke 'verkeersagent' en kan niet de inhoud van de informatie lezen.

Als identificatie van een gebruiker wordt als basis een pseudoniem gebruikt, een voor de gebruiker niet zichtbare betekenisloze cijferreeks dat via het inlogmiddel automatisch wordt gegenereerd. Kenmerkend is dat voor dezelfde gebruiker voor elke dienstaanbieder een ander pseudoniem wordt gegenereerd. Op deze wijze kunnen dienstaanbieders op basis van alleen deze identificatie geen informatie relateren aan dezelfde persoon (geen profiling).

Tijdens het inloggen kan een publieke of private dienstaanbieder optioneel vragen om aanvullende persoonsgegevens, zoals een naam of emailadres. Het is dan aan de gebruiker om toestemming te verlenen om die aanvullende persoonsgegevens ook te verstrekken. Datzelfde geldt ook voor authenticaties in het private domein. Bijvoorbeeld bij het online kopen van een bioscoopkaartje kan worden volstaan met alleen het verstrekken van een pseudoniem en kan het bioscoopkaartje als pdf worden geprint. Het pseudoniem wordt wel bewaard, dat is handig als de gebruiker weer toegang wil krijgen tot zijn bestelde bioscoopkaartjes. De bioscoop kent alleen het pseudoniem van de gebruiker en is daarmee voor de bioscoop anoniem. De Wet bescherming persoonsgegevens (Wbp) is ook hier van toepassing.

Toepassing in het publieke domein

Voor de online toegang tot de dienstverlening van burgers in het publieke domein, kiest de overheid ervoor om de standaardisatie vorm te geven door middel van het beschrijven van een uniform eisenpakket waaraan de inlogmiddelen en de leveranciers van die middelen moeten voldoen. Daarmee wordt het mogelijk dat burgers toegang krijgen tot de publieke dienstverlening niet alleen met inlogmiddelen die door de overheid worden uitgegeven (aangeduid als publieke inlogmiddelen), maar ook met daarvoor toegelaten private inlogmiddelen. Het wordt dan voor de gebruiker mogelijk om inlogmiddelen te kiezen die voor hem vertrouwd zijn en passen bij zijn gebruiksvoorkeur.

Deelname pilots

De gebruiker heeft bij private inlogmiddelen de keuze voor het middel dat de gebruiker het prettigst vindt. De gebruikers die deelnemen aan de pilots met private inlogmiddelen worden door de leverancier van dat middel op de hoogte gesteld van de werkwijze.

<u>Pilots met private middelen: Idensys</u>
De gebruiker kan tijdens de pilots inloggen bij deelnemende dienstverleners. De gebruiker ziet daar, naast de mogelijkheid om in te loggen, een Idensys-knop. Als de gebruiker daar op klikt, kan hij (net als bijvoorbeeld iDEAL) kiezen voor de leverancier van zijn private middel. Vervolgens kan de gebruiker met zijn middel inloggen. Via een openbare procedure op Tenderned zijn de leveranciers geattendeerd op de mogelijkheid zich aan te melden voor deelname aan de pilots en alleen leveranciers die door de certificering van de overheid komen, worden toegelaten.

<u>Pilot met private middelen: bankpilot</u>
De pilot bij de Belastingdienst betreft het indienen van de aangifte via het portaal MijnBelastingdienst. Om voor de pilot in te loggen in MijnBelastingdienst vindt de gebruiker, naast de Indensys-knop, nog een tweede pilot-knop om met behulp van een bankmiddel te kunnen inloggen. Hier volgt voor de gebruiker eenzelfde handelswijze als voor het inloggen bij de Idensys pilots: de gebruiker kiest zijn bank en logt vervolgens in.
De banken die meedoen aan deze pilot zijn de ABN AMRO bank, ING Bank, Rabobank, SNS Bank en Triodos Bank. Er kunnen maximaal 65.000 mensen gebruik maken van de inlogmogelijkheid met het bankenmiddel. Deelname is vrijwillig. Gebruikers die meedoen met de pilot kunnen zelf kiezen om gebruik te maken van de inlog via Idensys of via het bankenmiddel. Daarnaast blijft inloggen met DigiD uiteraard gewoon beschikbaar.

<u>Pilots met publieke inlogmiddelen: eNIK en eRijbewijs</u>
De deelnemers aan de pilots met het publieke eID-middel (de eNIK respectievelijk het eRijbewijs) maken gebruik van de Nederlandse Identiteitskaart die voor de pilot geschikt is gemaakt als eNIK of van (een specimen van) het eRijbewijs. Zij ontvangen van de betreffende gemeente Den Haag respectievelijk Eindhoven informatie over de werkwijze. De keuze voor het publieke eID-middel wordt toegevoegd aan het openingsscherm van DigiD, dus naast de huidige keuzes (gebruikerscode + wachtwoord / sms). Deelnemers aan de pilot met publieke inlogmiddelen ontvangen bij uitgifte (dat wil zeggen de identiteitskaart of specimen rijbewijs) een kaartlezer (hier zijn voor de deelnemers aan deze pilot geen kosten aan verbonden). Door gebruik te maken van die kaartlezer kunnen deelnemers aan de pilot straks inloggen met hun publieke eID-middel. De kaartlezer werkt contactloos door middel van de NFC technologie.[1]

[1] NFC staat voor Near Field Communication en is een contactloze communicatiemethode.

Privacy

In het AO van 25 november is geschetst welke maatregelen zijn getroffen om de privacy van deelnemers aan de pilots te waarborgen. In aanvulling daarop volgt hierbij een nadere toelichting op een aantal specifieke punten.

Makelaars
Door de VVD is gesteld dat makelaars in Idensys niet meer kunnen zijn dan 'verkeersregelaars'. Dit is een terechte constatering. Door het gebruik van pseudoniemen en versleuteling zijn zij inderdaad de 'verkeersagent' die doorverwijzen, maar niet over de inhoudelijke gegevens beschikken.

Recht op inzage van persoonlijke gegevens
Door het gebruik van pseudoniemen is het in het private domein niet mogelijk voor dienstverleners om gegevens onderling uit te wisselen. Dit beschermt de privacy van de gebruiker.

De gebruiker heeft recht op inzage conform de geldende privacy wet- en regelgeving. De Authenticatiedienst[2] zal dit inzicht gaan verzorgen, onder meer door inzicht te bieden in de vastgelegde gegevens en door hem uitgegeven authenticatiemiddelen.

Om inzage te krijgen in de eigen gegevens moet een gebruiker inloggen op een speciale inkijkpagina bij de authenticatiedienst. Daarvoor gebruikt hij/zij het middel dat de gebruiker bij de authenticatiedienst heeft.

Bewaartermijnen
In het Besluit verwerking persoonsgegevens GDI en de tijdelijke Regeling pilot e-Nik, wordt vastgelegd wat de bewaartermijnen zijn voor persoonsgegevens:

- De bewaartermijn van persoonsgegevens met betrekking tot het publieke middel in de pilots bedraagt, afhankelijk van het type gegevens, maximaal 18 maanden;[3]
- De bewaartermijn van persoonsgegevens in het BSN-koppelregister is ook (maximaal) 18 maanden, eveneens afhankelijk van het type gegevens.[4]

Beveiliging en Toegang

Voor diensten in het overheidsdomein kan men in de huidige situatie gebruik maken van het publieke middel DigiD, waarbij de dienstverlener het betrouwbaarheidsniveau bepaalt.[5] Er is behoefte voor de digitale dienstverlening aan middelen op een hoog en substantieel betrouwbaarheidsniveau (hiervoor was dit STORK 3 en 4). In het kader van de multimiddelenstrategie worden pilots uitgevoerd met betrouwbaarheidsniveau hoog en substantieel. Bij middelen op deze betrouwbaarheidsniveaus is er altijd sprake van een 'twee-factor' authenticatie.

[2] Een authenticatiedienst heeft als specifieke dienst het vaststellen van de identiteit van de gebruiker.

[3] Conform regeling pilots e-NIK -NIK

[4] Conform het bestluit (AMVB) verwerking persooonsgegevens GDI

[5] De eIDAS verordening kent drie betrouwbaarheidsniveaus: laag, substantieel en hoog, waarbij tijdens het vaststellen van de eisen die eraan gesteld zijn rekening gehouden is met de betrouwbaarheidsniveaus uit STORK en ISO 29115; zie UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015. Klik hier voor de link.

Eisen aan dienstverleners en private leveranciers tijdens pilots

Dienstverleners
Voor de dienstverleners gelden bestaande wet- en regelgeving op het gebied van elektronisch bestuurlijk berichtenverkeer, privacy en informatiebeveiliging. Zo mogen zij bijvoorbeeld alleen over die gegevens van de gebruiker beschikken die noodzakelijk zijn voor het doel waarvoor ze worden verwerkt (doelbinding) en er moeten passende technische en organisatorische beveiligingsmaatregelen worden genomen. Ook zijn dienstverleners gehouden aan de beveiligingsrichtlijnen van het NCSC.

Eisen aan private leverancier zijn:

- pilots met private middelen in het publieke domein op basis van het afsprakenstelsel Idensys:
  - de inhoudelijke eisen en verplichtingen voor de private leveranciers zijn te vinden onder Afsprakenstelsel Elektronische Toegangsdiensten;
- Voor pilots met bankmiddelen geldt de DNB regelgeving.[6]

Publiek Middel tijdens pilots

De Nederlandse Identiteitskaart (NIK) en het rijbewijs zijn standaard uitgerust met een chip. Op deze kaarten staan altijd een basissysteem en één of meer applets; kleine programma's die bepalen voor welke functies de kaart geschikt is. Dit is enigszins vergelijkbaar met een telefoon waarop apps worden geladen – maar dan op veel kleinere schaal en strenger beveiligd.

Voor de pilot wordt een applet geplaatst naast de bestaande NIK en rijbewijs applets. De techniek van deze applet is Public Key Infrastructure (PKI): de applet bevat een sleutel waarmee kan worden aangetoond dat het om een originele kaart gaat en niet om een kopie. Voor de pilots wordt gebruik gemaakt van gecertificeerde chips.

Om de kaart te kunnen gebruiken om in te loggen is net zoals met private middelen een authenticatiedienst nodig. Voor de pilot wordt de bestaande authenticatiedienst van DigiD gebruikt, met de bestaande aangesloten dienstaanbieders.

De techniek voor het publieke eID-middel is vergelijkbaar met het systeem in België, alleen wordt in de Nederlandse pilot gebruik gemaakt van DigiD als authenticatiedienst, terwijl in België de server van de dienstaanbieder direct communiceert met de kaart (dus zonder tussenkomst van een authenticatiedienst).

Voor pilots met publieke middelen geldt bestaande regelgeving vanuit BZK

[6] BankID Control Framework "acceptance criteria for issuing parties".

Buitenlandse overheden

Tijdens het AO zijn vragen gesteld over de uitwisseling van gegevens naar buitenlandse mogendheden en in het bijzonder de Amerikaanse. In een brief aan uw Kamer op 24 november 2014,[7] is uiteengezet hoe de Patriot Act zich verhoudt tot Europese en Nederlandse wetgeving.

De Patriot Act vergt medewerking van onder Amerikaanse rechtsmacht vallende bedrijven om in bepaalde omstandigheden door hen verwerkte persoonsgegevens over te dragen aan Amerikaanse autoriteiten ten behoeve van terrorismebestrijding. Deze Amerikaanse wetgeving kan door extraterritoriale effecten in de uitvoering spanning opleveren met EU-wetgeving die in Nederland is geïmplementeerd in de Wet bescherming persoonsgegevens. Deze wetgeving stelt eisen aan internationale doorgifte van persoonsgegevens vanuit Nederland door diezelfde bedrijven. Ook kunnen aanbieders van software en hardware ten behoeve van ICT-netwerken, of bedrijven die worden ingeschakeld om netwerken te bouwen of onderhouden, directe of indirecte banden hebben met de Verenigde Staten.

In deze brief staat: "Het kabinet vindt de mogelijkheid dat bedrijven met conflicterende plichten te maken kunnen krijgen onwenselijk. Het zet daarom ten eerste in op het zoveel als mogelijk beperken van nadelige gevolgen door afspraken in contracten. Het kabinet voelt zich in deze aanpak gesteund door een recente rechterlijke uitspraak.[8] De contractuele voorwaarden moeten overigens telkens ook worden gelezen in het licht van nieuwe aanscherpingen van het gegevensbeschermingsrecht door de Europese rechter, zoals de verplichting tot opslag van persoonsgegevens op EU-grondgebied.[9] Daarbij zet het kabinet zich ook bij de onderhandelingen over de algemene verordening gegevensbescherming in voor het verkleinen van het risico op conflicterende plichten.[10] Het kabinet is zich er echter van bewust dat het moeilijk, zo niet onmogelijk zal zijn om hier een volledig sluitende oplossing te bereiken, gegeven de aard van de problematiek. De weg die we via Europa bewandelen om de dialoog te zoeken met de Verenigde Staten om over verschillende onderwerpen te onderhandelen is de enige manier waarop we met respect voor elkaars rechtsstelsel tot oplossingen kunnen komen."[11]

[7] Kamerstuk 26643 nr. 337, gepubliceerd op 3 december 2014.
[8] Zie Rechtbank Midden-Nederland, Vereniging Praktijkhoudende Huisartsen [VPH] v. Vereniging van Zorgaanbieders voor zorgcommunicatie [VZVH], 23 juli 2014, ECLI:NL:RBMNE:2014:3097 (uitspraak elektronisch patiëntendossier), r.o. 5.40.
[9] Zie de uitspraak van het Hof van Justitie van 8 april 2014 jl. in Digital Rights Ireland en Seitlinger, C-293/12 en C294/12, waarin expliciet wordt verduidelijkt dat uit het vereiste van onafhankelijk toezicht door een gegevensbeschermingsautoriteit op bescherming en beveiliging van persoonsgegevens voortvloeit dat deze gegevens op EU-grondgebied moeten worden bewaard (r.o. 68).
[10] Kamerstuk 22 112, nr. 1372, blz. 7.
[11] Kamerstuk 26643 nr. 337, gepubliceerd op 3 december 2014.

Bijlage II: Hoofdlijnen Uniforme Eisen Elektronische Toegangsdiensten

Dit hoofdstuk bevat een beschrijving van de onderwerpen die nader zullen worden uitgewerkt in het toegezegde uniforme pakket van eisen waaraan moet worden voldaan door leveranciers van authenticatiemiddelen om deze te kunnen laten gebruiken in het publieke domein. Het betreft de eisen voor authenticatiemiddelen ten aanzien van betrouwbaarheid, veiligheid, privacy, techniek, toezicht, beheer en governance die op termijn eenduidig zullen worden vastgelegd in wet- en regelgeving.[12]

Voor de te stellen eisen zal worden uitgegaan van de inhoud van de normenkaders uit het Afsprakenstelsel Elektronische Toegangsdiensten,[13] BankID Control Framework[14] en de regelgeving inzake DigiD.[15] De onderwerpen die aan de orde komen zijn:

1. Beheer

   In dit onderdeel wordt ingegaan op beheer(processen), het algemene niveau van dienstverlening dat wordt gehanteerd en de wijze waarop communicatie-uitingen worden vormgegeven.

2. Techniek en functionaliteit

   In dit onderdeel wordt een beschrijving gegeven van de koppelvlakspecificaties, de use cases en testen voor leveranciers van middelen. Het bevat eisen mbt te hanteren (open) standaarden, de functionaliteit, de berichten en koppelvlakken die worden ondersteund en de testen die worden uitgevoerd.

3. Informatiebeveiliging

   In dit onderdeel zijn de eisen opgenomen ten aanzien van veiligheid en de maatregelen die worden genomen om het vertrouwen in en de continuïteit van de voorzieningen en het netwerk te borgen.

4. Privacy
   Dit gaat over de maatregelen die de bescherming van de persoonlijke levenssfeer betreffen (verwerking van persoonsgegevens, bewaartermijnen, verstrekkingen, etc.).

5. Toezicht

   Hier wordt de wijze van toezicht beschreven.

6. Governance

   Hier wordt de wijze van besturing beschreven.

[12] Zie Brief over Uitgangspunten Wetgeving GDI, https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/documenten/kamerstukken/2015/12/04/kamerbrief-over-uitgangspunten-wetgeving-generieke-digitale-infrastructuur
[13] Zie Afsprakenstelsel Elektronische Toegangsdiensten - https://afsprakenstelsel.etoegang.nl/display/as/Startpagina
[14] BankID Cotnrol Framework “acceptance criteria for issuing parties”.
[15] Thans gereguleerd op basis van de Wet Elektronisch Berichtenverkeer Belastingdienst in de Regeling Voorzieningen GDI http://wetten.overheid.nl/BWBR0037124/geldigheidsdatum_09-12-2015